BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

ABSTRACTED-PUB-NO: JP09046672A

BASIC-ABSTRACT:

The apparatus has a scramble key with extractor having and encrypted encipherment device which changes and boosts a scrambler (3). A

de-scrambler is included in a decoder (31) which decodes the encrypted scramble key changed by the encipherment device.

ADVANTAGE - Enables careless decoding of scramble key. Prevents excessive use of scramble key.

CHOSEN-DRAWING: Dwg.1/5

TITLE-TERMS: APPARATUS BROADCAST STATION DECODE DECODE ENCRYPTION SCRAMBLE KEY CHANGE BOOST DEVICE

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平９－４６６７２

(43)公開日　平成９年（１９９７）２月１４日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04N 7/16			H04N 7/16	A	
H04H 1/00			H04H 1/00	F	

審査請求　未請求　請求項の数２　ＯＬ　（全７頁）

(21)出願番号　特願平７－１９１４４９

(22)出願日　平成７年（１９９５）７月２７日

(71)出願人　０００００２１８５
ソニー株式会社
東京都品川区北品川６丁目７番３５号

(72)発明者　吉田　洋之
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　城間　真
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

(72)発明者　山下　雅美
東京都品川区北品川６丁目７番３５号　ソニー株式会社内

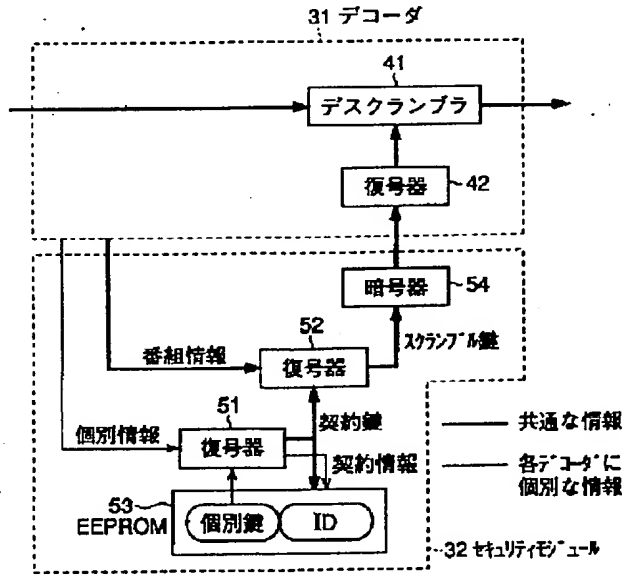
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】デスクランブル装置および方法

(57)【要約】

【課題】　スクランブル鍵が盗用されるのを抑制する。

【解決手段】　デコーダ３１に対して装着されるＩＣカードなどよりなるセキュリティモジュール３２に、暗号器５４を設ける。この暗号器５４により、スクランブル鍵を暗号化してデコーダ３１に出力する。デコーダ３１においては、復号器４２で、この暗号化されたスクランブル鍵を復号化し、デスクランブラ４１に供給する。デスクランブラ４１は、復号器４２より供給されたスクランブル鍵を用いて、スクランブルされているデータをデスクランブルする。



受信端末 22

1

【特許請求の範囲】

【請求項１】　放送されてきた複数の情報を分離するとともに、スクランブルされている所定のチャンネルの番組の情報をデスクランブルするデスクランブル手段と、前記デスクランブル手段に対して着脱され、放送されてきた情報から前記スクランブルを解除するためのスクランブル鍵を抽出し、前記デスクランブル手段に供給する抽出手段とを備えるデスクランブル装置において、

前記抽出手段は、前記スクランブル鍵を暗号化して前記スクランブル手段に供給する暗号化手段を備え、

前記デスクランブル手段は、前記暗号化手段により暗号化された前記スクランブル鍵を、復号化する復号化手段を備えることを特徴とするデスクランブル装置。

【請求項２】　放送されてきた複数の情報を分離するとともに、スクランブルされている所定のチャンネルの番組の情報をデスクランブルするデスクランブル手段と、前記デスクランブル手段に対して着脱され、放送されてきた情報から前記スクランブルを解除するためのスクランブル鍵を抽出し、前記デスクランブル手段に供給する抽出手段とを備えるデスクランブル装置のデスクランブル方法において、

前記抽出手段において、前記スクランブル鍵を暗号化して前記スクランブル手段に供給し、

前記デスクランブル手段において、暗号化された前記スクランブル鍵を、復号化することを特徴とするデスクランブル方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デスクランブル装置および方法に関し、特にスクランブル鍵が不用意に解読され、不正に利用されるのを抑制するようにしたデスクランブル装置および方法に関する。

【０００２】

【従来の技術】有料放送においては、スクランブル放送と呼ばれる放送方式が用いられることが多い。このスクランブル放送は、放送局側において、元の信号を所定の方法で意図的に乱す（スクランブルする）ことにより、放送局と契約していない者が放送を受信しても、正常な画像、音声、およびデータなどを利用することができないようにするものである。

【０００３】すなわち、放送局と契約した者のデコーダに対しては、このスクランブルを解除する鍵信号を与え、この鍵信号によりデコーダがスクランブルされているデータを元の形にデスクランブルすることで、正常な画像、音声、およびデータなどを得ることができるようにしている。

【０００４】有料放送を視聴する契約のうち、チャンネル単位で契約する場合をフラット、視聴した番組に応じて課金される場合をペイパービューという。ペイパービューのうち、視聴者が急に所定の番組を見たくなった場

2

合、所定の操作を行うだけでそれを見ることができる、事前連絡が不要のものを特にインパルスペイパービューといい、事前連絡が必要なものを、コールアヘッドペイパービューという。

【０００５】

【発明が解決しようとする課題】このように、スクランブル放送をデスクランブルするには、鍵信号が必要となるが、従来のスクランブル装置においては、この鍵が不正に取得され、視聴契約をしていない者が、スクランブル放送を不正に視聴するおそれがあった。

【０００６】本発明はこのような状況に鑑みてなされたものであり、視聴契約をしていない番組が、不正に視聴されることを抑制するものである。

【０００７】

【課題を解決するための手段】請求項１に記載のデスクランブル装置は、抽出手段は、スクランブル鍵を暗号化してスクランブル手段に供給する暗号化手段を備え、デスクランブル手段は、暗号化手段により暗号化されたスクランブル鍵を、復号化する復号化手段を備えることを特徴とする。

【０００８】請求項２に記載のデスクランブル方法は、抽出手段において、スクランブル鍵を暗号化してスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化することを特徴とする。

【０００９】請求項１に記載のデスクランブル装置においては、抽出手段が、スクランブル鍵を暗号化してスクランブル手段に供給する暗号化手段を備え、デスクランブル手段が、暗号化手段により暗号化されたスクランブル鍵を、復号化する復号化手段を備える。

【００１０】請求項２に記載のデスクランブル方法においては、抽出手段において、スクランブル鍵を暗号化してスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化する。

【００１１】

【発明の実施の形態】図１は、本発明を応用した有料放送システムの一実施例の構成を示すブロック図である。送信側システム２１のエンコーダ１（１Ａ乃至１Ｅ）は、５チャンネル分の映像信号や音声信号をディジタル化し、圧縮するようになされている。多重化器２は、複数（５チャンネル分）のエンコーダ１の出力や複数の関連情報をパケット化し、時分割多重する。ここで関連情報とは、番組に関する情報とデスクランブルのためのスクランブル鍵を含む「共通情報（番組情報）」、加入者（視聴者）毎の契約情報（例えばフラットやペイパービューなどの契約形態など）および共通情報の暗号を解くための契約鍵を含む「個別情報」などからなるものとする。

【００１２】スクランブラ３は、関連情報送出装置４からのスクランブル鍵により、多重化器２の出力信号の所

定のものに対して選択的にスクランブルを施すようになされている。

【００１３】スクランブル制御システム６は、関連情報送出装置４に契約鍵（ワーク鍵）を供給するとともに、受信端末２２に固有の個別鍵（スクランブル制御システム６に記憶されている）により契約鍵を暗号化し、個別情報の一部として多重化器２に供給するようになされている。

【００１４】関連情報送出装置４は、スクランブラ３にスクランブル鍵を供給するとともに、スクランブル制御システム６から供給された契約鍵により、スクランブル鍵を暗号化し、共通情報（番組情報）の一部として多重化器２に供給するようになされている。

【００１５】番組制御システム５は、所定の制御信号を発生し、番組に応じてエンコーダ１を制御する。すなわち、デジタル化や圧縮の方法を制御する。また、いま、エンコーダ１においてエンコードされている番組の番組ＩＤや対応するチャンネルのチャンネルＩＤ（ｓｅｒｖｉｃｅ－ｉｄ）等を発生し、関連情報送出装置４に供給する。視聴情報収集処理システム７は、多数の受信端末２２から電話回線２４を介してアップロードされる視聴情報（例えば視聴した番組ＩＤ、対応するチャンネルＩＤ、および視聴した時間など）や、視聴者からの契約要求を処理し、契約情報としてスクランブル制御システム６に供給するようになされている。

【００１６】一方、受信端末２２のデコーダ３１（デスクランブル手段）は、内蔵するデスクランブラ４１（図４）により、セキュリティモジュール３２（抽出手段）から供給されたスクランブル鍵により、スクランブルされた信号を元の信号にデスクランブルするようになされている。また、番組に付加された個別情報や番組情報を抽出し、出力するようになされている。

【００１７】セキュリティモジュール３２は、デコーダ３１に対して着脱自在に装着される例えばＩＣカード等により構成され、内蔵するＥＥＰＲＯＭ５３（図４）に、受信端末２２に固有の個別鍵を記憶しており、デコーダ３１よりスクランブルされていない個別情報が供給されたとき、この個別鍵を用いて個別情報を復号し、契約鍵と契約情報をそれぞれ取り出し、記憶する。また、デコーダ３１を介して供給された番組に付随する共通情報を取り込み、契約鍵により共通情報を復号し、スクランブル鍵を取り出し、暗号化した後、デコーダ３１に供給するようになされている。

【００１８】次にその動作について説明する。まず、送信側システム２１より受信端末２２に個別情報が送信される場合の動作について説明する。この個別情報は、図２に示すように、契約鍵に対応する契約鍵番号、契約鍵、契約したチャンネルに対応するチャンネルＩＤ（ｓｅｒｖｉｃｅ－ｉｄ）、および契約タイプなどを含んでいる。また、個別情報は、送信先の受信端末２２のＩＤ番号（Ｃａｒｄ　ＩＤ）も含んでいる。

【００１９】契約鍵は、例えば、８ビットの契約鍵番号とともに送信され、複数の契約鍵を使い分けることができるようになっている。契約したチャンネルＩＤを、例えば１６ビットのＳｅｒｖｉｃｅ＿ｉｄで表すものとする。契約タイプは、フラット、ペイパービュー、特別契約を識別することができるもので、例えば４ビットとする。

【００２０】この個別情報は、スクランブル制御システム６において、この個別情報が送信されるべき送信先の受信端末２２に固有の個別鍵を用いて暗号化される。スクランブル制御システム６は、全ての受信端末２２について、受信端末２２に固有の個別鍵を受信端末２２のＩＤ番号（Ｃａｒｄ　ＩＤ）に対応させて記憶しており、送信先の受信端末２２のＩＤ番号からその個別鍵を検索することができるようになっている。従って、送信先の受信端末２２のＩＤ番号に対応する個別鍵を検索し、それに基づいて、個別情報が暗号化されることになる。暗号化された個別情報は多重化器２に供給される。

【００２１】多重化器２においては、エンコーダ１より供給された所定の番組に対応するディジタル化され、圧縮された映像信号や音声信号と、スクランブル制御システム６より供給された個別情報がパケット化され、時分割多重された後、スクランブラ３に供給される。スクランブラ３に供給されたディジタル信号は、関連情報送出装置４より供給されたスクランブル鍵を用いて番組部分（映像データと音声データ）だけがスクランブルされ、個別情報の部分はスクランブルされずに伝送路２３に送出される。

【００２２】なお、この個別情報の受信端末２２への送信は、個別情報の更新が必要とされる時に、必要に応じて随時行われる。この個別情報には、上述した契約情報が含まれている。

【００２３】次に、通常の番組とそれに付加された番組情報（共通情報の構成要素）が送信側システム２１から受信端末２２に送信される場合の動作について説明する。

【００２４】番組情報は、例えば図３に示すように、契約タイプ、契約鍵の番号を示す契約鍵番号、スクランブル鍵、チャンネルＩＤに相当するＳｅｒｖｉｃｅ＿ｉｄ、番組を識別するための番組ＩＤなどを含んでいる。このうちスクランブル鍵は、スクランブル制御システム６より供給された契約鍵（ワーク鍵）によって暗号化されている。また、契約タイプには、特別番組であるか否かを識別するためのフラグが含まれている。

【００２５】関連情報送出装置４において生成された上述したような構成の所定の番組情報は、多重化器２に供給される。多重化器２においては、エンコーダ１から供給された所定の番組に対応するディジタル化され、圧縮された映像信号や音声信号と、関連情報送出装置４より

供給された番組情報がパケット化され、時分割多重され、スクランブラ３に供給される。

【００２６】スクランブラ３には、番組を構成する圧縮された映像信号や音声信号と番組情報がパケット化され、時分割多重されたディジタル信号が入力されるが、このうちの番組部分（映像信号と音声信号）だけが関連情報送出装置４より供給されたスクランブル鍵によってスクランブルされ、番組情報の部分はスクランブルされずに伝送路２３に送出される。

【００２７】このようにして、所定の番組とそれに付随する番組情報が送信側システム２１より受信端末２２に送信される。

【００２８】次に、受信端末２２側の動作について説明する。

【００２９】図４は、受信端末２２において、視聴許可の制御を行う場合の原理的な動作を説明するための図である。デコーダ３１は、例えば、デスクランブラ４１と復号器４２（復号化手段）により構成され、セキュリティモジュール３２は、復号器５１，５２、ＥＥＰＲＯＭ５３および暗号器５４（暗号化手段）より構成されている。

【００３０】正式に契約した視聴者の受信端末２２には、個別情報が送信される。送信側システム２１より、伝送路２３を介して送信されたスクランブルされた所定の番組と、スクランブルされていない個別情報が時分割多重されたディジタル信号が、受信端末２２の図示せぬチューナにより受信されると、スクランブルされた番組に対応するディジタル信号は、デスクランブラ４１に供給される。

【００３１】一方、スクランブルされていない個別情報の非暗号部に付加された受信端末２２のＩＤ番号（Ｃａｒｄ　ＩＤ）と、セキュリティモジュール３２のＥＥＰＲＯＭ５３に予め記憶されている受信端末２２のＩＤ番号（Ｃａｒｄ　ＩＤ）とが比較され、両者が一致した場合、その個別情報が（すなわち自分自身宛の個別情報が）取り込まれ、復号器５１に供給される。

【００３２】復号器５１に供給された個別情報のうち、暗号化されている部分は、ＥＥＰＲＯＭ５３に記憶されている受信端末２２に固有の個別鍵によって解読され、契約鍵、および契約情報が取り出され、ＥＥＰＲＯＭ５３に供給され、記憶される。この契約鍵は、番組情報の解読に使用される。また、契約情報は、受信した番組が契約した番組であるか否かを判断するとき使用される。

【００３３】受信端末２２において、視聴者が番組を視聴しているとき、受信端末２２は、伝送路２３を介して送信されてきたスクランブルされた所定の番組と、それに付随した番組情報を受信している。スクランブルされた所定の番組に対応するディジタル信号は、デスクランブラ４１に供給され、それに付随した番組情報は、復号器５２に供給される。

【００３４】所定の番組のチャンネルに対応する契約鍵が、上述したようにして、すでに復号器５１において復号され、ＥＥＰＲＯＭ５３に記憶されている場合、復号器５２が動作し、ＥＥＰＲＯＭ５３より供給されたその契約鍵によって番組情報のうちの暗号化されている部分が復号化される。これにより、番組情報に含まれているスクランブル鍵が取り出される。

【００３５】復号器５２により復号化されたスクランブル鍵は、暗号器５４に入力され、暗号化される。この暗号化には、ＥＥＰＲＯＭ５３に記憶されているＣａｒｄ　ＩＤとＣａ＿Ｓｙｓｔｅｍ＿ＩＤ（これについては、後述する）の少なくとも一方が利用される。

【００３６】この場合、Ｃａｒｄ　ＩＤとＣａ＿Ｓｙｓｔｅｍ＿ＩＤの少なくとも一方を、そのまま暗号化のための鍵として用いたり、所定の演算を施すことにより、暗号化を行うことができる。

【００３７】次に、番組情報は、ＥＥＰＲＯＭ５３にすでに記憶している契約情報との照合が行われる。照合の結果、番組情報が付加された番組が、契約した番組であると認識された場合、暗号器５４において得られたスクランブル鍵（暗号化されている）は、セキュリティモジュール３２からデコーダ３１の復号器４２に供給される。

【００３８】デコーダ３１側においては、復号器４２が、入力された暗号化されているスクランブル鍵を復号化する。この復号化には、上述したように、セキュリティモジュール３２の暗号器５４において暗号化のために用いられたＣａｒｄ　ＩＤまたはＣａ＿Ｓｙｓｔｅｍ＿ＩＤが必要となるが、これらは図５を参照して後述するように、セキュリティモジュール３２をデコーダ３１に装着したとき、セキュリティモジュール３２からデコーダ３１に供給され、デコーダ３１側において、記憶されている。

【００３９】復号器４２は、復号したスクランブル鍵を、デスクランブラ４１に供給する。デスクランブラ４１においては、スクランブルされている所定の番組のディジタル信号が、復号器４２より供給されたスクランブル鍵（復号化されている）によってデスクランブルされ、正常に視聴可能な元の信号に戻された後、出力される。

【００４０】図４の実施例における暗号器５４と復号器４２を省略した構成にすると、セキュリティモジュール３２を他の装置で駆動し、その出力をメモリなどに取り込むようにすると、スクランブル鍵が第３者に不正に取得され、悪用されるおそれがある。しかしながら、実施例のように、暗号器５４により暗号化した状態でスクランブル鍵を出力するようにしておくと、セキュリティモジュール３２より出力されたスクランブル鍵を単に取り込んだだけでは、このスクランブル鍵は暗号化されているため、そのままでは用いることができない。従って、

スクランブル鍵の盗用を抑制することができる。

【００４１】なお、デコーダ３１は、これを分解すると、内部の回路が正常に動作しないように構成されていたり、分解すると、分解されたことが視聴情報としてＥＥＰＲＯＭ５３に記憶され、さらに視聴情報収集処理システム７に転送されるように構成されているので、デコーダ３１の分解により、スクランブル鍵が盗用されるおそれは抑制されている。

【００４２】次に、図５を参照して、ＩＣカードで構成されるセキュリティモジュール３２を、デコーダ３１に装着した場合に行われる動作について説明する。

【００４３】セキュリティモジュール３２は、独自に動作を行うことがなく、常にデコーダ３１からの指令に対応して、所定の返事を返す機能のみを有している。

【００４４】デコーダ３１は、セキュリティモジュール３２が装着されたとき、最初に、Ｒｅｓｅｔ信号を発生し、セキュリティモジュール３２に出力する。セキュリティモジュール３２は、このＲｅｓｅｔ信号が入力されると、リセット動作を行い、リセット動作が完了すると、Ａｎｓｗｅｒ　Ｔｏ　Ｒｅｓｅｔ信号をデコーダ３１に出力する。

【００４５】デコーダ３１は、このＡｎｓｗｅｒ　Ｔｏ　Ｒｅｓｅｔ信号の入力を受け、セキュリティモジュール３２のリセットが完了したことを検知すると、次に、セキュリティモジュール３２に対して、ＩＤ　Ｒequｅｓｔ信号を出力する。セキュリティモジュール３２は、このＩＤ　Ｒｅｑｕｅｓｔ信号の入力を受けたとき、ＥＥＰＲＯＭ５３に記憶されているＣａｒｄ　ＩＤとＣａ＿Ｓｙｓｔｅｍ＿ＩＤをデコーダ３１に出力する。

【００４６】このＣａｒｄ　ＩＤは、セキュリティモジュール３２に個別に与えられたセキュリティモジュール３２に固有のＩＤである。セキュリティモジュール３２は、受信した個別情報のうち、自分自身の個別情報として、ＥＥＰＲＯＭ５３に取り込むべき個別情報であるのか否かを判定するのに、このＣａｒｄ　ＩＤを用いている。

【００４７】一方、Ｃａ（Ｃｏｎｄｉｔｉｏｎａｌ　ａｃｃｅｓｓ）＿Ｓｙｓｔｅｍ＿ＩＤは、複数の限定受信システムが共存する場合において、各受信システムを識別するための識別子である。

【００４８】デコーダ３１は、このＣａｒｄ　ＩＤとＣａ＿Ｓｙｓｔｅｍ＿ＩＤが供給されたとき、これを内蔵するＲＡＭに記憶する。そして、上述したように、これらを復号器４２における復号の鍵として用いるようにする。

【００４９】次に、デコーダ３１は、受信した個別情報（ＥＭＭ：ＥｎｔｉｔｌｅｍｅｎｔＭａｎａｇｅｍｅｎｔ　Ｍｅｓｓａｇｅ）をセキュリティモジュール３２に出力する。セキュリティモジュール３２は、この個別情報（ＥＭＭ）の入力を受けたとき、Ｃａｒｄ　ＩＤに対応するものを抽出し、対応するＲｅｓｐｏｎｓｅをデコーダ３１に返す。

【００５０】また、デコーダ３１は、番組情報（ＥＣＭ：Ｅｎｔｉｔｌｅｍｅｎｔ　Ｃｏｎｔｒｏｌ　Ｍｅｓｓａｇｅ）を、セキュリティモジュール３２に出力する。セキュリティモジュール３２は、供給された番組情報から、上述したように、スクランブル鍵Ｋｓを復号し、これをさらに暗号化して、デコーダ３１に出力する。

【００５１】セキュリティモジュール３２は、スクランブル鍵Ｋｓ以外にも、Ｃｏｐｙ　ＲｉｇｈｔとＦｉｎｇｅｒ　Ｐｒｉｎｔｉｎｇを、デコーダ３１に出力する。このＣｏｐｙ　Ｒｉｇｈｔは、対応する番組をコピーすることが許可されているか否かを表すフラグである。また、Ｆｉｎｇｅｒ　Ｐｒｉｎｔｉｎｇは、その番組に対応されているＣａｒｄ　ＩＤを強制的にモニタに表示させるか否かを表すフラグである。

【００５２】以下、デコーダ３１より個別情報（ＥＭＭ）が供給されると、セキュリティモジュール３２は、それに対応するメッセージを返し、また、デコーダ３１より番組情報（ＥＣＭ）が供給されると、セキュリティモジュール３２は、対応するメッセージを返す動作が適宜行われる。

【００５３】上記実施例においては、伝送路２３を放送波であるものとして説明したが、これに限定されるものではなく、光ファイバケーブルやその他の伝送媒体とすることも可能である。

【００５４】また、暗号器５４と復号器４２で用いる鍵としては、Ｃａｒｄ　ＩＤまたはＣａ＿Ｓｙｓｔｅｍ＿ＩＤ以外のものを用いることも可能である。ただし、これらを用いれば、これらはセキュリティモジュール３２からデコーダ３１に最初に必ず伝送されるものなので、他の鍵を設定した場合のように、その鍵を伝送するシーケンスを新たに追加する必要がない。

【００５５】

【発明の効果】請求項１に記載のデスクランブル装置および請求項２に記載のデスクランブル方法によれば、抽出手段において、スクランブル鍵を暗号化してデスクランブル手段に供給し、デスクランブル手段において、暗号化されたスクランブル鍵を、復号化するようにしたので、スクランブル鍵が不用意に解読され、悪用されるのを抑制することができる。

【図面の簡単な説明】

【図１】本発明を応用した有料放送システムの構成例を示すブロック図である。

【図２】個別情報の一部を示す図である。

【図３】番組情報の一部を示す図である。

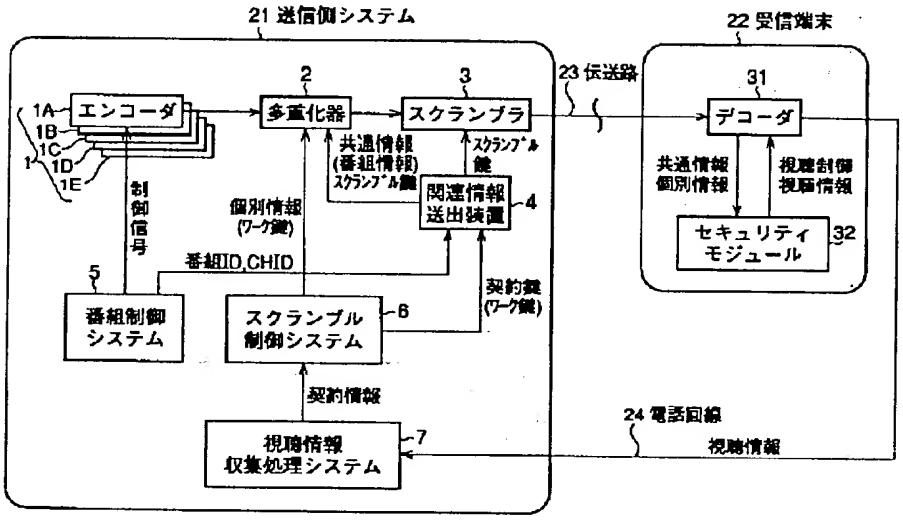
【図４】図１の受信端末２２の動作の原理を説明するための図である。

【図５】図１のデコーダ３１とセキュリティモジュール３２の間の信号の授受を説明する図である。

【符号の説明】

１，１Ａ乃至１Ｅ　エンコーダ
２　多重化器
３　スクランブラ
４　関連情報送出装置
５　番組制御システム
６　スクランブル制御システム
７　視聴情報収集処理システム
２１　送信側システム
２２　受信端末
２３　伝送路
２４　電話回線
３１　デコーダ
３２　セキュリティモジュール
４１　デスクランブラ
４２，５１，５２　復号器
５３　ＥＥＰＲＯＭ
５４　暗号器

【図１】



【図２】

契約鍵番号	契約鍵	service_id	契約ﾀｲﾌﾟ
8ビット	64ビット	16ビット	4ﾋﾞｯﾄ

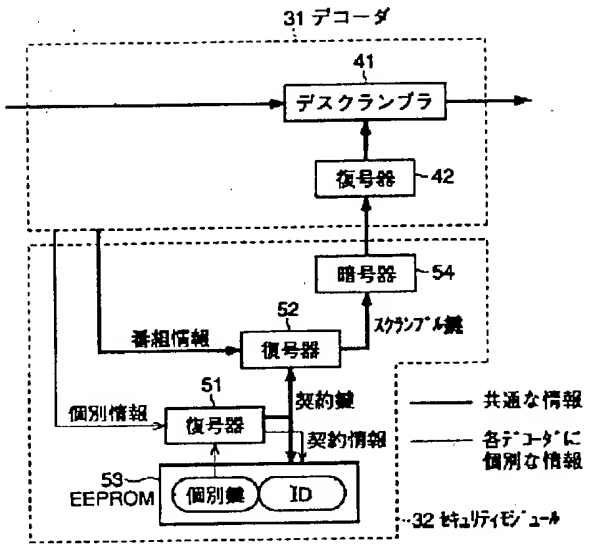
個別情報

【図３】

契約ﾀｲﾌﾟ	契約鍵番号	スクランブル鍵(暗号化)	service_id	番組ID
4ﾋﾞｯﾄ	8ビット	64ビット	16ビット	16ビット

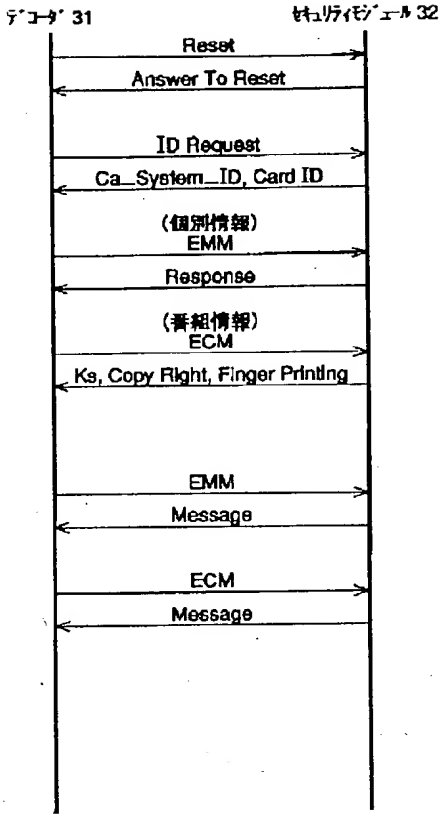
番組情報

【図４】


31 デコーダ
41
デスクランブラ
復号器
42
暗号器
54
52
スクランブル鍵
番組情報
復号器
51
契約鍵
個別情報
復号器
契約情報
59
EEPROM
個別鍵
ID
32 セキュリティモジュール
共通な情報
各デコーダに個別な情報

受信端末 22

【図５】


デコーダ 31
セキュリティモジュール 32
Reset
Answer To Reset
ID Request
Ca_System_ID, Card ID
(個別情報)
EMM
Response
(番組情報)
ECM
Ks, Copy Right, Finger Printing
EMM
Message
ECM
Message

This Page Blank (uspto)